МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

«На правах рукопису»
УДК 681.3.06

«До захисту допущено»
Завідуючий кафедрою СІКЗ
_____к.т.н. Г.В. Шуклін
«____» _____2023 р.

БАКАЛАВРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 “Кібербезпека”

на тему: **ОРГАНІЗАЦІЯ ЗАХИСТУ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ**

Студентка групи СЗД-41 Кукушкін Олександр Олегович _____
(підпис)

Науковий керівник: к.т.н., доц Шуклін Герман Вікторович _____
(підпис)

Нормоконтроль ст. викл. Зозуля Сергій Анатолійович _____
(підпис)

КИЇВ – 2023

«ЗАТВЕРДЖУЮ»
Завідувач кафедри СІКЗ
_____ к.т.н. Г.В. Шуклін
(підпис)
«_____»_____ 2023р.

ЗАВДАННЯ

на атестаційну роботу бакалавра

студенту: Кукушкіну Олександру Олеговичу

1.Тема роботи: Організація захисту електронного документообігу, затверджено наказом від «24 » лютого 2023р. № 26

2.Термін здачі студентом оформленої роботи «____» _____ 2023р.

3. Об'єкт дослідження: процеси захисту інформації при електронному документообігу.

4. Предметом дослідження: технології захисту, які забезпечують електронний документообіг.

5. Мета роботи: удосконалення та рекомендації щодо застосування методів захисту інформації при реалізації електронного документообігу.

6.Перелік питань, які мають бути розроблені:

Для досягнення вказаної мети виконуються такі основні задачі:

- аналіз проблеми захисту інформації при реалізації електронного документообігу;
- аналіз та дослідження існуючих методів захисту інформації при реалізації електронного документообігу.;
- створення рекомендацій щодо захисту інформації при реалізації електронного документообігу.

7. Дата видачі завдання «____» _____20____р.

Науковий керівник _____ Шуклін Г.В.
(підпис)

Завдання прийняла до виконання _____ Кукушкін О.О.
(підпис)

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання «24» лютого 2023р.

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури	до 26.02.23р.	
2	Обґрунтування актуальності теми роботи	до 27.02.23р.	
3	Написання першого розділу роботи	до 16.03.23р.	
4	Написання другого розділу роботи	до 12.04.23р.	
5	Написання третього розділу роботи	до 08.05.23р.	
6	Написання висновків по роботі	до 11.05.23р.	
8	Підготовка демонстраційних матеріалів	до 18.05.23р.	
9	Підготовка доповіді	до 24.05.23р.	
10	Захист в ДЕК		

Студент: СЗД -41 Кукушкін О.О. _____
(підпис)

Науковий керівник: к.т.н., доц. Шуклін Г.В. _____
(підпис)

Нормоконтроль: ст. викл. Зозуля С.А. _____
(підпис)

ЗМІСТ

РЕФЕРАТ

Дипломна робота містить 46 сторінок, 26 рисунки, 1 таблиць.

В даній атестаційні роботі запропоновано ескіз схеми забезпечення міжнародного значущого електронного документообігу для компаній холдингового типу, що діють у різних юрисдикціях. Показано варіанти забезпечення довіри до електронних сервісів, що надаються в різних локаціях. Виявлено найбільш значущі ризики інформаційної безпеки та запропоновано заходи їх зниження. Отриманий результат може бути застосований на практиці для забезпечення юридичної значущості електронних документів для транскордонного інформаційного обміну, зокрема для компаній, що діють у різних юрисдикціях.

Об’єктом дослідження: процеси захисту інформації при реалізації документообороту.

Предметом дослідження є технології захисту, які забезпечують безпеку передачі та прийому інформації при реалізації електронного документообороту.

Мета роботи удосконалення та рекомендації щодо застосування методів захисту інформації при реалізації документообороту для компаній холдингового типу.

Для досягнення вказаної мети виконуються такі основні задачі:

- аналіз існуючих підходів щодо захисту інформації при реалізації електронного документообігу;
- аналіз та дослідження існуючих методів захисту інформації при реалізації електронного документообігу;
- створення рекомендацій щодо підвищення інформаційного захисту при реалізації електронного документообігу.

ABSTRACT

Thesis contains 46 pages, 23 figures, 1 tables

This certification paper proposes a sketch of a scheme for ensuring internationally significant electronic document flow for holding companies operating in different jurisdictions. Options for ensuring trust in electronic services provided in different locations are shown. The most significant information security risks are identified and measures to reduce them are proposed. The result obtained can be applied in practice to ensure the legal significance of electronic documents for cross-border information exchange, in particular for companies operating in different jurisdictions.

Object of research: information security processes in the implementation of document management.

The subject security technologies that ensure the safe transmission and reception of information when implementing electronic document management.

The purpose Improvements and recommendations on the use of information security methods in the implementation of document management for holding companies.

To achieve this goal, the following main tasks are performed:

- analysis of existing approaches to information security in the implementation of electronic document management;
- analysis and research of existing methods of information protection in the implementation of electronic document management;
- development of recommendations for improving information security in the implementation of electronic document management.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

СЕД	Система електронного документообігу	
ОІД	Об`єкт інформаційної діяльності	
СІЗ	Системи інформаційного захисту	
EEPROM	Постійний запам’ятовувач що програмується та очищується за допомогою електрики	
NIST	Національний інститут стандартизації та технологій	The National Institute of Standards and Technology
PKI	Інфраструктура публічних ключів	Public key infrastructure
RAM	Пам’ять з довільним доступом	Random Access Memory
RFID	Радіочастотна ідентифікація	Radio frequency identification
ROM	Пам’ять лише для читання	Read Only Memory
SRAM	Статична оперативна пам’ять з довільним доступом	Static random access memory
TDMA	Метод часового поділу	Time division multiple access
WLAN	Метод часового поділу	Wireless Local Area Network
ВЧ	Високі частоти	
ЗЗІ	Засоби захисту інформації	
ІС	Інформаційна система	
ІТС	Інформаційно-телекомунікаційна система	
ОЗП	Оперативний запам’ятовувальний пристрій	
УВЧ	Ультра високі частоти	

ВСТУП

Механізми захисту інформації систем електронного документообігу (СЕД) реалізуються на засадах комплексного підходу до організації захисту і враховують розмаїття можливих загроз інформаційній безпеці СЕД, а також величину можливих втрат від реалізованих загроз. Захист інформації в СЕД полягає не тільки в захисту інформації електронних документів та розподілу доступу до них.

Актуальність теми У сучасному суспільстві оперативність ухвалення рішень та їхня подальша реалізація допомагають підприємству в досягненні поставлених стратегічних і тактичних цілей, що, своєю чергою, є найважливішими чинником успішної роботи підприємств.
При прискоренні зростання обсягів інформації, необхідної для забезпечення комерційної діяльності, перехід підприємств до електронного документообігу та електронної звітності дає їм низку переваг. Однією з таких переваг є функціонування підприємства в єдиному інформаційному просторі. Крім того, забезпечується електронний облік і зберігання документів, що є ефективнішим, порівняно з аналогічною формою звітності на паперових носіях. Отже, створення надійно захищеної системи захисту електронного документообігу є актуальним завданням сьогодення.

Об’єктом дослідження: процеси захисту інформації при реалізації документообороту.

Предметом дослідження є технології захисту, які забезпечують безпеку передачі та прийому інформації при реалізації електронного документообороту.

Мета роботи удосконалення та рекомендації щодо застосування методів захисту інформації при реалізації документообороту для компаній холдингового типу.

Для досягнення вказаної мети виконуються такі основні задачі:

- аналіз існуючих підходів щодо захисту інформації при реалізації електронного документообігу;

- аналіз та дослідження існуючих методів захисту інформації при реалізації електронного документообігу;
- створення рекомендацій щодо підвищення інформаційного захисту при реалізації електронного документообігу.

РОЗДІЛ 1 ПРОЕКТУВАННЯ ЗНАЧУЩОГО ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

1.1. Рішення електронного документообігу в Україні

На теперішній час в Україні доступна значна кількість СЕД, які володіють різним функціоналом. За основу було взято реалізовану раніше СЕД, а підготовчим етапом проекту є апробація електронного документообороту для українських компаній холдингового типу в 2022 році. Проект планувався з урахуванням розвитку під міжнародною системою документообороту і вже на початковій стадії давав змогу обмінюватися електронними документами (ЕД) у рамках єдиної інформаційної системи в усіх країнах присутності підрозділів компанії холдингового типу. Цей проект СЕД став переможцем конкурсу «Системи електронного документообороту в Україні» в номінації "Найкращий регіональний проект у Центральній і Східній Європі". Надалі реалізований раніше проект перед початком реалізації додаткового функціоналу та значного розгортання в різних юрисдикціях пройшов глибинну експертизу порівняно з наявними аналогами.

На першому етапі проекту міжнародної системи електронного документообігу вихідна сукупність наявних систем пройшла першу фільтрацію за наступною системою критеріїв:

- систематизація роботи з ЕД;
- підготовка документів за уніфікованими (стандартними) формами;
- автоматична класифікація за різними параметрами;
- автоматизація пошуку;
- здійснення розсилки та ознайомлення з опублікованими ЕД;
- колективний доступ до ЕД;
- використання централізованого сховища для зберігання ЕД і метаданих; - формування звітів, зокрема статистики; - робота зі списком персональних доручень.

Після першого фільтра сукупність, що залишилася, пройшла фінальне оцінювання за такими критеріями:

- за ступенем інтеграції з прикладним програмним забезпеченням;
- вартість володіння в перерахунку на 1 документ у мінімальному тарифі;
- режим роботи служби технічної підтримки;
- мінімальна вартість інтеграції з СЕД на рік;

У підсумку серед найкращих залишилися системи: *Контур.Діадок*, *Такском*, *СБІС*, *Synerdocs*. Надалі під час виконання ескізного проектування міжнародної системи електронного документообігу було обрано одну з найбільших систем, що має найкращі показники за всіма критеріями і надає необхідний список сервісів електронного підпису (ЕП). Важливо зазначити додатково, що під час формування фінального рішення щодо вибору оператора ЕП було враховано ризики, які було підготовлено представниками служби безпеки, служби документообігу, а також юридичного і технічного департаментів. Деталі формування критерію оцінювання ризиків ґрунтуються на "*класичних*" стандартах *ISO* серії 31000 та *ISO* серії 27005.

1.2.Формування технічного завдання

Для компаній холдингового типу, що діють у різних юрисдикціях, реалізацію сервісів міжнародної системи документообігу має підтримувати серйозна технічна інфраструктура, зокрема з урахуванням перспективних технологій та обмежень обчислювальної потужності наявної серверної IT-інфраструктури. Також було детально розглянуто, зокрема, специфічні вимоги митного законодавства, електронного нотаріату та додатків *ECommerce*. Було сформовано основні вимоги для технічного завдання оператору ЕП, таких як

- сервер оператора ЕП має внутрішній інтерфейс та зовнішній інтерфейс, які забезпечують сервіси міжнародної системи електронного документообігу для резидентів України та не резидентів, тобто іноземним компаніям на єдиній базі систем комплексного захисту інформації *Crypto*Pro;

- сервіси міжнародної системи електронного документообігу оператора

забезпечують ЕП для довільних типів електронних документів від контрагентів - резидентів до контрагентів - нерезидентів і у зворотному напрямку;
- сервіси МЕДО Оператора забезпечують логи за підсумками аналізу УКЕП від контрагентів (резидентів) і НЕП контрагентів (нерезидентів), підписані УКЕП Оператора;
- інтеграція внутрішньої ІТ-інфраструктури та сервісів МЕДО Оператора має бути максимально "безшовною", орієнтуватися на наявні корпоративні рішення документообігу, бухгалтерії, фінансових додатків, засобів захисту інформації;
- реалізація проекту має забезпечувати максимальну можливість розширення функціоналу внутрішньої ІТ-інфраструктури без критичних взаємозв'язків із сервісами міжнародної системи електронного документообігу оператора;
- реалізація проекту має найбільшою мірою зберігати реалізований нормативно-методичний базис бухгалтерських та фінансових додатків, облікову політику, внутрішні регламенти інформаційної безпеки;
- реалізація проекту має враховувати платформо-незалежність і максимальний ступінь імпортозаміщення.

Загальну схему побудови міжнародної системи електронного документообігу відповідно до сформованого технічного завдання на рисунку 1.1 представлено загальну її схему.

Рисунок 1.1. Загальна схема побудови міжнародного документообігу.

На схемі не показано УЦ, мається на увазі, що він включений у захищену IT-інфраструктуру Оператора. Питання резервування елементів критичної IT-інфраструктури Оператора та офісів компаній холдингового типу, що діють у різних юрисдикціях, не показано. Передбачається забезпечення рівного ступеня довіри для будь-якого офісу компанії холдингового типу в будь-якій юрисдикції.

1.3.Ескізнє проектування

Після формування технічного завдання на етапі ескізного проектування було розглянуто кілька варіантів реалізації сервісів міжнародної системи електронного документообігу за участю оператора. Для компаній холдингового типу, що діють у різних юрисдикціях, пропонувались наступні варіанти: ***Варіант 1.*** Кожен контрагент забезпечується *СКЗІ CryptoPro* завдяки придбанню через оператора для резидентів - звичайної версії, для нерезидентів - в експортному виконанні. Інформаційний обмін відбувається за єдиним

технологічним режимом: *СКЗІ CryptoPro* та алгоритми ЕП та шифрування - ДСТЗУ. "*Ланцюжоу довіри*" встановлюється УЦ оператора.

Варіант 2. Кожен контрагент серед резидентів забезпечується *СКЗІ CryptoPro* завдяки закупівлі через оператора, а для нерезидентів рекомендується перелік *СКЗІ*, які підтримують зарубіжні алгоритми ЕП шифрування (*RSA*, *ECDSA*). Інформаційний обмін відбувається за комбінованим технологічним режимом: *СКЗІ CryptoPro* від резидентів до оператора (*ДСТЗУ*) і від нерезидента до оператора (*RSA*, *ECDSA*). Оператор відіграє роль *ДТС*, засвідчуючи і *УКЕП* (*ДСТЗУ*), і *НЕП* (*RSA*, *ECDSA*). "*Ланцюжок довіри*" встановлюється УЦ оператора.

Варіант 3. Кожен контрагент серед резидентів забезпечується *СКЗІ CryptoPro* через закупівлю через оператора, а для нерезидентів рекомендується перелік *СКЗІ*, які підтримують зарубіжні алгоритми ЕП та шифрування (*RSA*, *ECDSA*), додатково реалізується посередник "*крипто – хаб*", який реалізується *СКЗІ CryptoPro* завдяки закупівлі через оператора для нерезидентів у вигляді експортного варіанту. Інформаційний обмін здійснюється за комбінованим технологічним режимом: *СКЗІ CryptoPro* від резидентів до оператора (*ДСТЗУ*), далі від оператора до "*крипто – хаб*" і далі - від нерезидентів до оператора (*RSA*, *ECDSA*). Тепер "*крипто – хаб*" відіграє роль *ДТС*, засвідчуючи *НЕП* (*ДСТЗУ*) і *НЕП* (*RSA*, *ECDSA*). "*Ланцюжокдовіри*" встановлюється від *УЦ* оператора до "*крипто – хаб*", ЕП якого простежується до визнаних світових постачальників. Загальну схему побудови міжнародної системи електронного документообігу для компаній холдингового типу на стадії ескізного проектування представлено на рисунку 1.2.

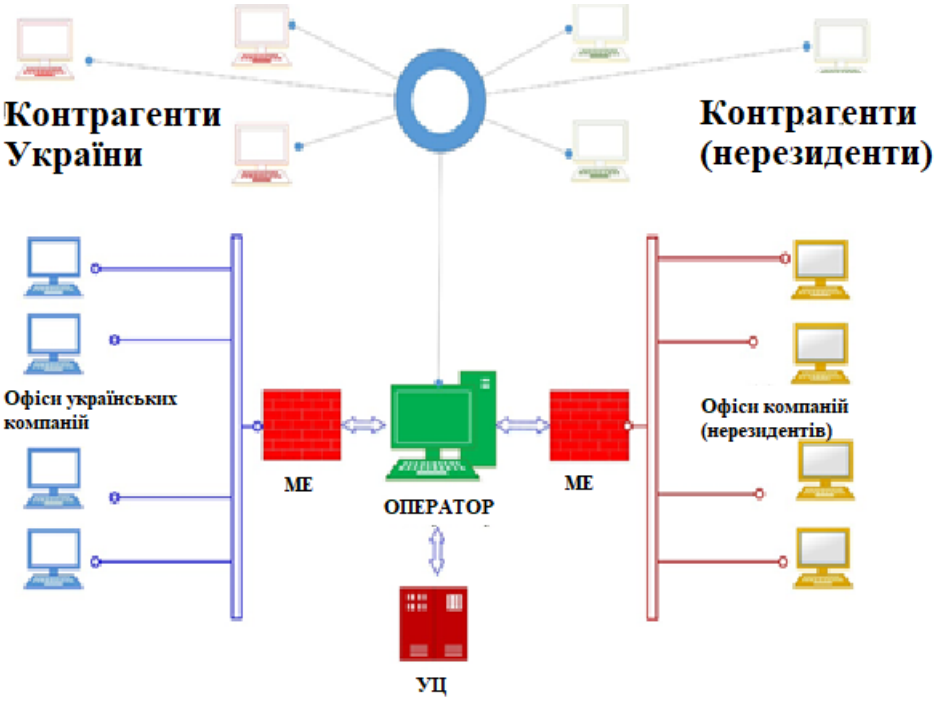


Рисунок 1.2. Загальна схема побудови міжнародної системи електронного документообігу для компаній холдингового типу.

На стадії ескізного проектування додатково було вивчено такі аспекти:

- відповідність застосовним вимогам різних юрисдикцій у частині ЕП;
- захист "одного ступеня міцності" для внутрішніх і/або зовнішніх інтерфейсів;
- орієнтація на вітчизняні *СІКЗ* для формування ЕП та шифрування;
- забезпечення миттєвого і безпечного обміну електронного документу за встановленими (резервними) каналами зв'язку для всіх офісів компанії холдингового типу;
- розділення функцій безпеки та адміністратора в периметрі компанії холдингового типу;
- забезпечення надійного та безпечного тривалого архівного зберігання електронного документу.

Додатково слід зазначити, що увага до сервісів документів архівного зберігання зараз значно зросла, оскільки сервіси міжнародної системи електронного документообігу дедалі більше набувають практичного застосування, при цьому кількість електронних документів, які пройшли обробку може обчислюватися нескінченною кількістю.

На етапі ескізного моделювання було ідентифіковано, проаналізовано і визнано значущими такі ризики:

- коректне оцінювання контексту ЕД для користувачів у різних юрисдикціях ("context" мається на увазі в нотації ISO як сукупність соціальних, культурних, політичних, правових, регуляційних, фінансових, технологічних, економічних та інших чинників на міжнародному, національному, регіональному або місцевому рівнях);

- виявлення актуальних загроз і кількісне оцінювання ризиків (у нотаціях ISO, NIST, Cobit) для IT-інфраструктури в периметрі компанії холдингового типу;

- повна і достовірна валідація кінцевих пристроїв (встановлене системне і прикладне ПЗ, засоби захисту, з двох факторів автентифікація, СКЗІ тощо);

- авторизацію доступу до сервісів МЕДО в периметрі компанії холдингового типу; - забезпечення і відновлення стійкості (Resilience).

Загальну схему побудови МЕДО для компаній холдингового типу на стадії ескізного проектування у варіанті 1 з "*крипто – хабом*" представлено на рисунку 1.3.

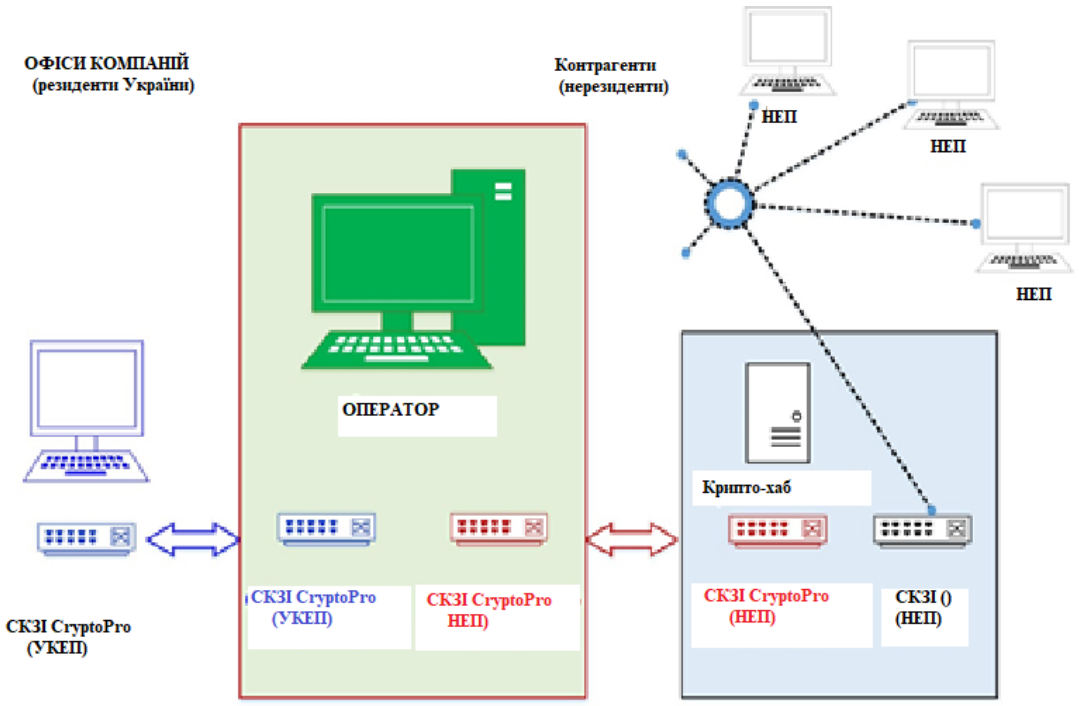


Рисунок 1.3. Загальна схема побудови міжнародної системи електронного документообігу для компаній холдингового типу з "*крипто – хабом*".

1.4.Апробація

Апробація ескізного проекту відбулася на XVIII міжнародній конференції з проблематики інфраструктури відкритих ключів та електронного підпису PKI-Форум (https://ib-bank.ru/pki-forum/materials2020) у 2020 р. у межах двох самостійних доповідей, представлених авторами. У процесі дискусії було обговорено наукові та науково-практичні особливості проведеного ескізного етапу проекту і, загалом, отримано схвалення спільноти провідних експертів у цій галузі.

Висновок до розділу 1

1.В даному розділі проведено аналіз правових, організаційних та технічних аспектів забезпечення міжнародного значущого електронного документообігу для компаній холдингового типу, що діють у різних юрисдикціях.

2.Показано варіанти забезпечення довіри до електронних сервісів, що надаються в різних локаціях. Виявлено найбільш значущі ризики інформаційної безпеки та запропоновано заходи їх зниження.

3.Самою перспективною видається схема за варіантом № 3 з окремим "*крипто – хабом*", що має низку важливих переваг: гнучка та безшовна інтеграція з усіма корпоративними IT-Системами, застосуванням вітчизняних засобів автоматизації та ефективних засобів криптографічного захисту інформації, здатних забезпечувати безпечний обмін документами в компанії холдингового типу.

4.Отриманий результат може бути застосований на практиці для забезпечення юридичної значущості електронних документів для транскордонного інформаційного обміну, зокрема для компаній, що діють у різних юрисдикціях.

РОЗДІЛ 2 ОСОБЛИВОСТІ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

2.1. Математична модель

Нині спостерігається тенденція переходу паперового документообігу до електронного, що зумовлює інтенсивність розвитку автоматизованих інформаційних систем електронного документообігу (АІС ЕД), у зв'язку з чим виникає потреба в захисті даних (електронних документів), які в них обробляються.

Відповідно до чинного стандарту з управління документами, електронні документи (ЕД) складаються з контенту та метаданих, які описують їхні характеристики.

Рисунок 2.1. Структура електронного документу та функції його метаданних

Метадані є критично важливими для забезпечення значущості, збереженості та керованості ЕД, оскільки є описом характеристик даних у базах даних та електронних сховищах. Саме тому велике значення в управлінні документами необхідно приділяти механізму захисту метаданих в АІС ЕД.
З метою глибшого розуміння проблеми захисту метаданих необхідно в їхній загальній класифікації виокремити параметри, що залежать від часу: метадані можуть бути як статичними, так і динамічними. Відповідно до чинних нормативних документів, вони мають найменування метаданих введення документів у систему і метаданих процесів управління документами. Метадані введення документів у систему є статичними і є лише мінімально необхідним набором елементів, що ідентифікують ЕД у момент його створення, не відображаючи зміни змісту, структури та контексту документа протягом подальшого часу, що може бути представлено в алгебраїчному вигляді наступним чином

$$D(t_i) = K(t_i) \bigcup \left(\bigcup_{j=0}^{i} Z(t_j) \right), \tag{2.1}$$

де $K(t_i)$ - контент ЕД, який існує та модифікований в момент часу t_i, $Z(t_i)$ - метаданні, $D(t_i)$ - інформаційний блок, який уявляє собою ЕД. І задані початкові умови

$$D(t_0) = K(t_0) \bigcup Z(t_0) \ , \tag{2.2}$$

де t_0 - момент створення ЕД. На рисунку 2.2. представлено модель формування метеданних електронного документу.

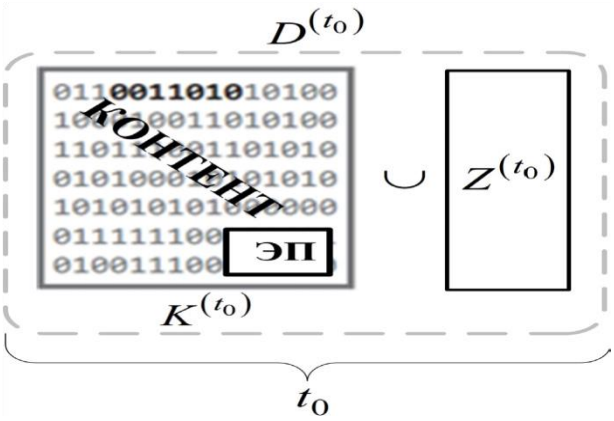


Рисунок 2.2. Структура моделі формування метаданних ЕД.

Призначення метаданих діловодних документів не вичерпується цілями пошуку інформації та потребує наявності шару динамічних метаданих з таких причин.

По-перше, офіційний управлінський документ повинен мати метадані, що відображають операції управлінської діяльності, тобто контекст створення, отримання та використання документа і зв'язки між його окремими компонентами. Такі метадані особливо необхідні для контролю статусу, структури та цілісності документа в будь-який певний час, а також для показу його зв'язків з іншими документа.

По-друге, метадані повинні документувати управлінський контекст, зміст, структуру та подання документа не тільки в момент створення документа або включення його в систему, а й після цього документувати управлінські процеси, в яких записи постійно використовуються, включаючи зміни у змісті, структурі та поданні.

Згідно представлення (2.1), зміни ЕД з урахуванням формування динамічних метаданих, в алгебраїчному вигляді можуть бути представлені як:

$$D(t_1) = K(t_1) \bigcup Z(t_1)$$

$$D(t_2) = K(t_2) \bigcup \left(Z(t_1) \bigcup Z(t_2) \right)$$

$$\ldots\ldots\ldots\ldots\ldots\ldots \qquad (2,3)$$

$$D(t_n) - K(t_n) \bigcup \left(\bigcup_{i-1}^{n} Z(t_i) \right)$$

де n - скінченний момент часу редагування електронного документу.

На рисунку 2.3 представлено структуру моделі формування динамічних метаданих ЕД.

Таким чином, метадані надають ЕД додаткової цінності, що робить управління метаданими одним із найважливіших процесів управління документацією організації. При цьому, керуючись вимогами вищеназваного стандарту, необхідно зазначити, що метаданими документа слід керувати, як керувати і самим документом, оскільки вони мають бути захищені від втрати або несанкціонованої зміни чи видалення та збережені або знищені відповідно до встановлених вимог.

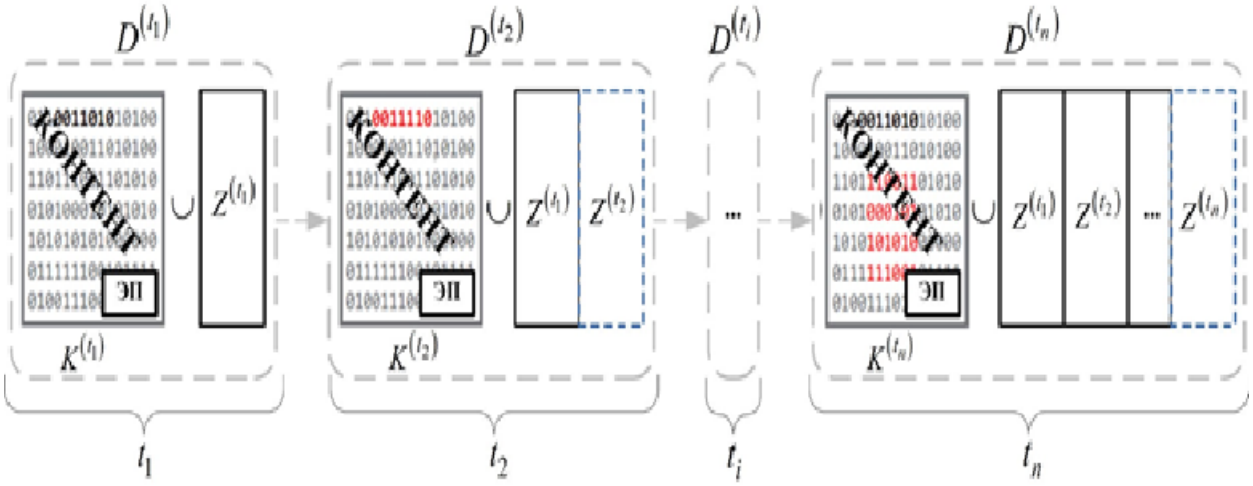


Рисунок 2.3. Структура моделі формування динамічних метаданих ЕД.

Метадані введення документів у систему формуються на етапі створення контенту ЕЛД (статичні) і фіксуються в реєстраційно-контрольній картці документа (РККД), а потім продовжують накопичуватися й доповнюватися протягом усього життєвого циклу ЕЛД, здійснюючи, таким чином, фіксацію процесів керування документами (динамічні). Зберігання контенту і РККД до нього в межах встановлених термінів забезпечує підсистема зберігання, що являє собою локальну базу даних (ЛБД), пошук необхідної інформації в якій здійснюється за допомогою метаданих, що містяться в РККД. Механізми захисту інформації, що зберігається в ЛБД, забезпечує підсистема захисту інформації. При цьому метадані, що містяться в РККД, і контент ЕЛД захищають за допомогою розмежування доступу до документів бази даних, а захист контенту ЕЛД, крім того, забезпечують засобами електронного підпису (ЕП), при цьому

вплив на контент ЕЛД може чинити тільки автор, а на РККД - усі, хто виконує функції агента .

На рис. 2.4 представлено наявну модель захисту ЕЛД, що обробляються АІС ЕД. до реквізитної частини не вносилося жодних змін.

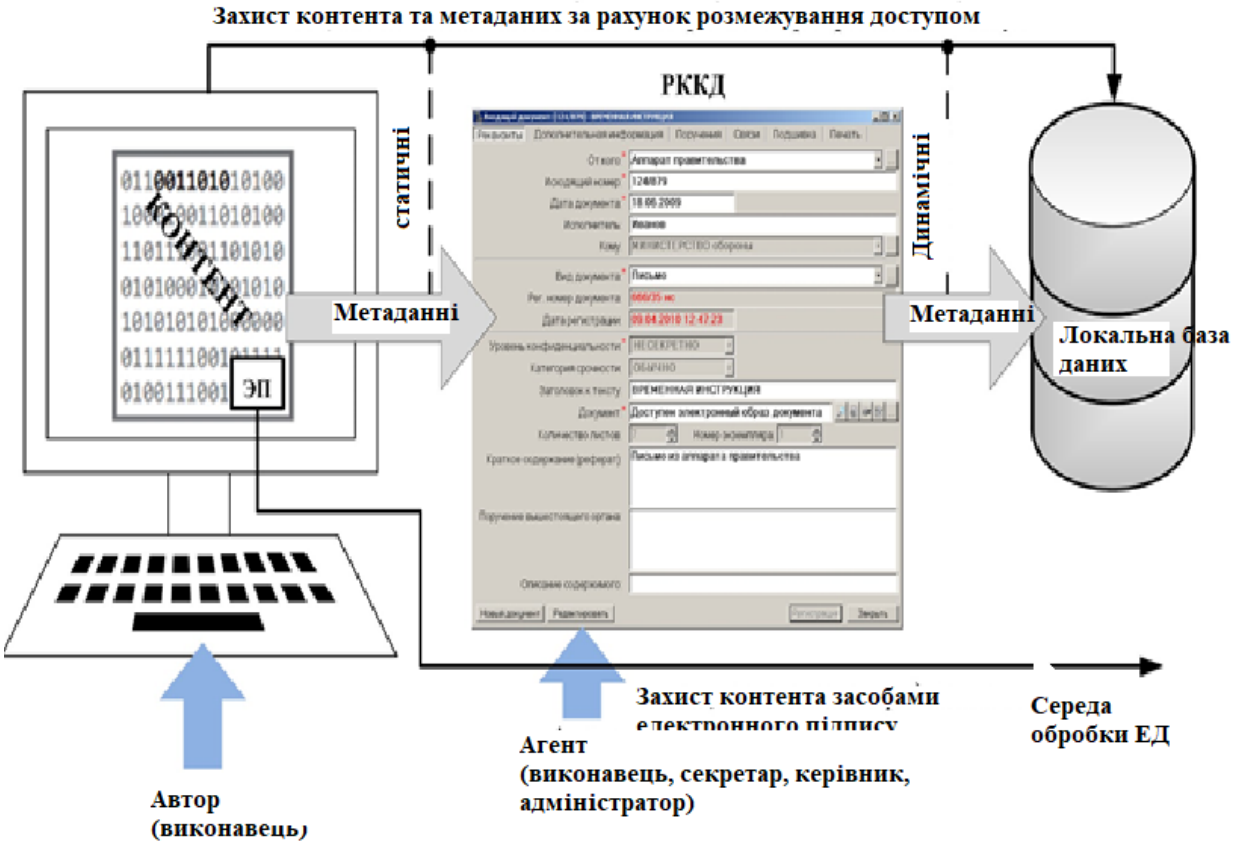


Рисунок 2.4. Існуюча модель захисту електронних документів

На практиці, цілісність ЕД визначається збігом хеш-кодів відправленого та отриманого ЕД, тобто цілісністю файлу ЕД. При цьому в основі алгоритмів електронного підпису (ЕП) лежать криптографічні методи, засновані на використанні математичних функцій, які просто обчислювати в одному напрямку і важко в іншому, тобто односторонні функції.

Водночас єдиним механізмом забезпечення захисту метаданих ЕД є функція розмежування доступу до ЛБД, у якій здійснюється їх зберігання. Таким чином, цей факт спричиняє розбіжність із положеннями чинних нормативних документів з управління документами, що виражається в надійнішому захисті

тільки контенту документа у відриві від його метаданих, що суперечить самому визначенню складу ЕД.

Наслідком саме застосування ЕП, що ґрунтується на криптографічних методах, дає змогу забезпечити необхідний рівень довіри до ЕЛД і, як наслідок, його правовий статус . ЕП дозволяє забезпечити такі властивості ЕЛД:

1) цілісність документа;

2) автентифікацію джерела документа (авторство);

3) незаперечність автора від підписання документа;

4) захист документа від можливого підроблення.

Чинне законодавство дає таке визначення поняттю "цілісність" застосовно до документованої інформації:

цілісність документа - стан документа, за якого після його випуску ні в змістовну, ні в таку організацію захисту не є відповідні загрози інформаційній безпеці, які можуть бути спричинені діями зловмисника.

Аналіз загроз безпеці інформації в АІС показує, що до актуальних загроз належать внутрішні загрози, тобто навмисні несанкціоновані впливи уповноважених користувачів. Результатом таких впливів може стати навмисна несанкціонована зміна метаданих, що призведе до порушення їхньої цілісності, і, як наслідок, втрати управління над ЕЛД, які обробляє АІС13 . Одним із заходів забезпечення захищеності даних є захист їхньої цілісності.

Відомо, що криптографічні методи захисту інформації є найбільш надійним засобом захисту даних. Проведений аналіз наявних способів контролю цілісності даних дав змогу встановити, що в їхній основі лежить застосування криптографічної хеш-функції. Але найбільший інтерес для розв'язання вищеназваної проблеми з організації захисту метаданих ЕЛД, що обробляються АІС ЕД, представляє метод "одноразового запису", а також спосіб аутентифікації повідомлень HMAC .

У методі "одноразового запису" використовуються два ЕП для кожного запису, щоб один законний користувач, який має криптографічний ключ, не мав змоги стерти або модифікувати вже підписаний, тобто захищений запис, переписати і

додати підпис ще раз. Таким чином, кожен запис підписується користувачем і адміністратором системи як це показано на рисунку 2.5.

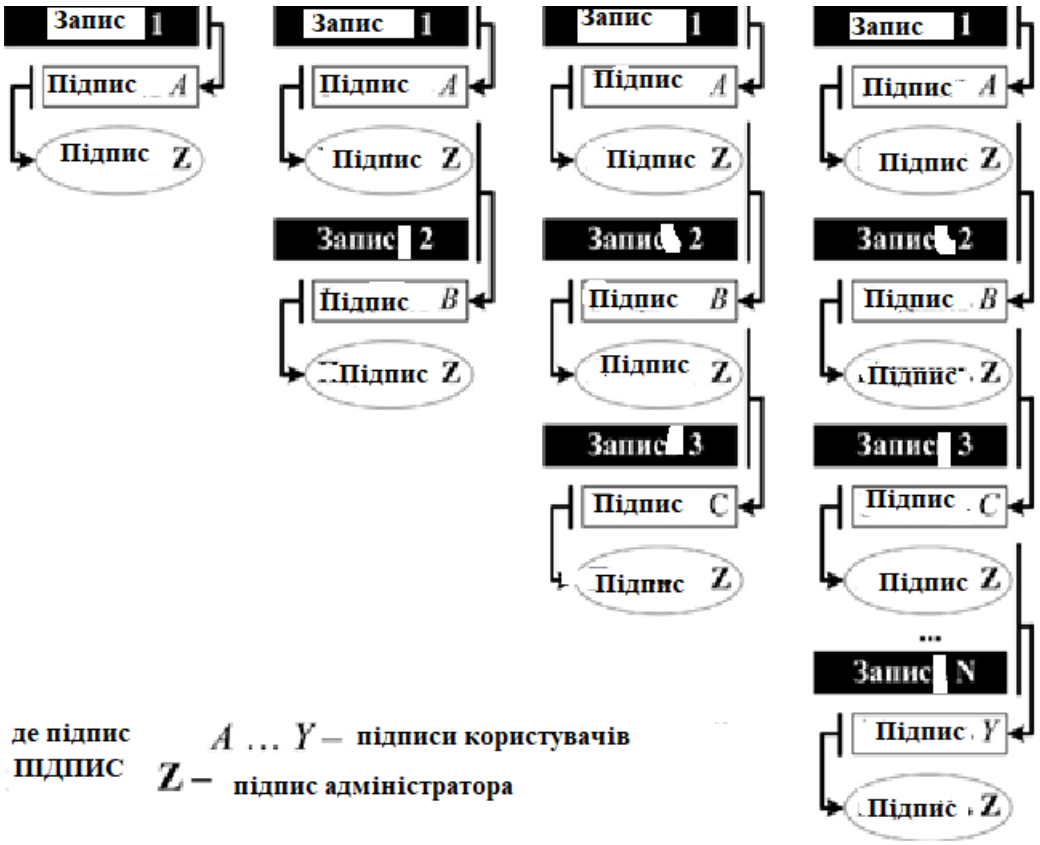


Рисунок 2.5. Схема функціонування методу «однократний запис».

Недоліком цього методу є той факт, що внутрішнім порушником може бути сам адміністратор. У способі автентифікації повідомлень HMAC, отриманий код автентичності дає змогу переконатися в тому, що дані не змінювалися жодним способом відтоді, як їх створило, передало або зберегло довірене джерело. Для такого роду перевірки необхідно, щоб, наприклад, дві сторони, які довіряють одна одній, заздалегідь домовилися про використання секретного ключа, який відомий тільки їм. Тим самим гарантується автентичність джерела і повідомлення, як це представлено на рисунку 2.6.

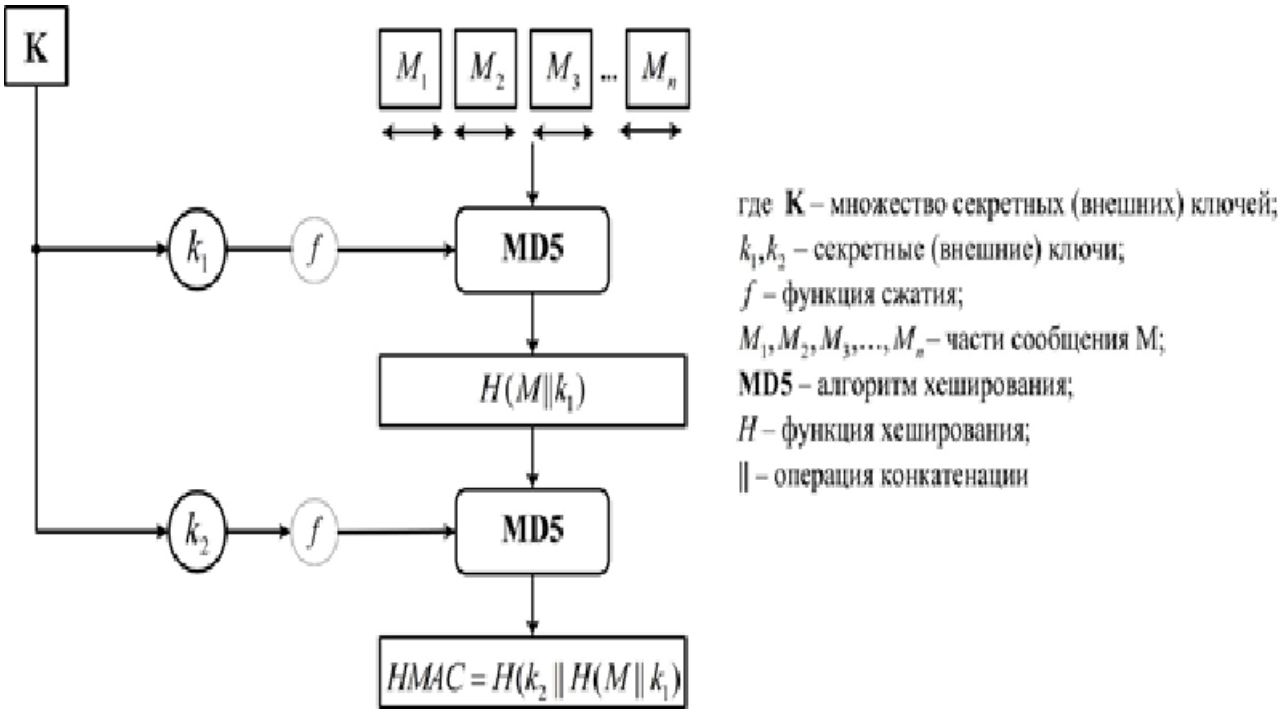


Рисунок 2.6. Схема функціонування способу аутентифікації повідомлень HMAC.

X - множина вхідних ініціювальних подій або впливів на підсистему ЗІ АІС ЕД;

Y - множина функціональних станів підсистеми ЗІ АІС ЕД;

R - множина вихідних якісних станів, які обробляються ЕЛД;

Z - множина метаданих ЕД, що змінюються під впливом ініціюючих подій або впливів.

Під час формалізації задачі дослідження необхідно, використовуючи математичний запис, сформулювати суть розв'язуваної задачі, критерій її розв'язування, вхідні та вихідні дані, суттєві чинники та умови задачі.

Для формалізованого опису підсистеми захисту інформації (ЗІ) АІС ЕД скористаємося теоретико-множинним підходом, що набув значного поширення під час опису різних технічних систем.

Дано:

Нехай задано математичну модель підсистеми ЗІ АІС ЕД: $S = \{T, X, Y, R, Z, \delta, \varphi\}$, де T - множина моментів часу, у які спостерігається підсистема ЗІ АІС ЕД, $t_i \in T$, $i = \overline{0,n}$, t_0 - початок експлуатації АІС ЕД, t_n - кінець експлуатації АІС ЕД; підсистему ЗІ АІС ЕД;

δ - оператор переходів, що відображає механізм зміни функціонального стану Y підсистеми АІС ЕД. Зміни функціонального стану Y підсистеми ЗІ АІС ЕД під впливом внутрішніх і зовнішніх ініціюючих подій X;

φ - оператор виходів, що описує механізм формування вихідних параметрів R ЕЛД, як реакції підсистеми ЗІ АІС ЕД на внутрішні та зовнішні ініціювальні події X.

Оператори δ і φ реалізують відображення:

$$\delta : TxXxY \to Y; \tag{2.4}$$

$$\varphi : TxXxY \to R. \tag{2.5}$$

Усякий стан R ЕД характеризується в кожний момент часу $t_i \in T$ множиною метаданих Z, що змінюються під впливом ініціювальних подій, що впливають X на підсистему ЗІ АІС ЕД. Як ініціювальні події, тобто впливи, X розглядають запити уповноважених користувачів на виконання деякої функції, що реалізує деструктивні впливи на метадані ЕД.

Обмеженням моделі підсистеми ЗІ АІС ЕД є те, що елементи множини R містять тільки два стани: "1" - стан ЕД, за якого цілісність метаданих забезпечено; "0" - стан ЕД, за якого цілісність метаданих порушено, що може бути записано як

$$R(Y, Z(X)) = \begin{cases} 1 - \textit{стан цілісності метаданих ЕД} \\ 0 - \textit{стан порушення цілісності метаданих ЕД} \end{cases}.$$

Перехід ЕД у процесі функціонування підсистеми ЗІ АІС ЕД у стан "0" слід розглядати як подію, що характеризує порушення функціонування АІС ЕД. Водночас знаходження ЕЛД у стані "1" слід розглядати як подію, що характеризує стан нормального функціонування АІС ЕД.

У загальному випадку ймовірність забезпечення цілісності ЕЛД, що обробляється АІС ЕД, визначається наступним представленням:

$$P_{(1)} = \prod_{k=1}^{n} P_{(1)}^{(k)}, \quad (2.6)$$

де $P_{(1)}^{(k)}$ - імовірність забезпечення цілісності ЕД під час реалізації k-ї ініціювальної події X, які реалізуються у підсистемі ЗІ АІС ЕД; n - загальна кількість ініціювальних подій X, що реалізуються в підсистемі ЗІ АІС ЕД. Відповідно, імовірність порушення цілісності ЕЛД, що обробляється АІС ЕД, визначається представленням:

$$P_{(0)} = 1 - P_{(1)}. \quad (2.7)$$

У цьому випадку критерій якості функціонування підсистеми ЗІ АІС ЕД визначатиметься наступною умовою:

$$P_{(0)} < P_{порог}, \quad (2.8)$$

де $P_{порог}$ задається вимогами тактико-технічного завдання замовника.

Виходячи з чого, як показник ефективності функціонування підсистеми ЗІ АІС ЕД візьмемо ймовірність порушення цілісності ЕД $P_{(0)}$, викликаної за допомогою деструктивних впливів уповноважених користувачів на метадані ЕД. З урахуванням наявного стану справ як критерій оцінювання рівня захищеності метаданих ЕЛД розглядається така умова:

$$G : P_{(0)} < P_{(0)}^{прототипа} \quad (2.9)$$

де $P_{(0)}^{прототипа}$ - імовірність порушення цілісності прототипу ЕД, викликана за допомогою деструктивних впливів уповноважених користувачів на метадані ЕлД при використанні відомих способів контролю цілісності даних (хеш-функція).

Потрібно розробити такий спосіб контролю цілісності метаданих ЕД $Q = \{Md, Al, Mt\}$, що складається з моделей Md, алгоритмів Al і методики Mt, який дасть змогу за вихідних даних знайти вектор Y^* безлічі функціональних станів підсистеми ЗІ АІС ЕД, який за заданих обмежень дасть змогу підвищити рівень захищеності G метаданих ЕД, оброблюваних АІС ЕД.

В математичному формулюванні задача має наступне представлення:

$$Q: \arg\left(R\left(Y^{*}, Z(X)\right)\right) \rightarrow P_{(0)}\left(R\left(Y, Z(X)\right)\right) < P_{(0)}^{прототипа} \qquad (2.10)$$

Як обмеження $C(F_{допустимий}, T_{заданні})$ можуть виступати вимоги:

- ресурс, що витрачається, не перевищує допустимого $F_{допустимий}$;

- витрати часу не перевищують директивних $T_{задані}$.

На підставі проведеного аналізу наявних способів контролю цілісності даних, з метою усунення виявлених недоліків було ухвалено рішення використовувати технологію ланцюгового запису даних, що являє собою реєстр, дані до якого записуються блоками, таким чином, що кожен новий блок містить інформацію про попередній блок.

Під реєстром розуміють сукупність даних, структурованих і збережених з метою їхнього обліку, пошуку, опрацювання та контролю, якими і є метадані ЕЛД. Причому допускається внесення інформації в блоки (записи метаданих) без зміни раніше внесеної інформації, що являє собою динамічний реєстр. При цьому зв'язок із блоками (записами метаданих) буде забезпечуватися за рахунок використання криптографічної хеш-функції. Стосовно завдання підвищення захищеності метаданих технологія ланцюгового запису даних має вигляд, як показано на рисунку 2.7.

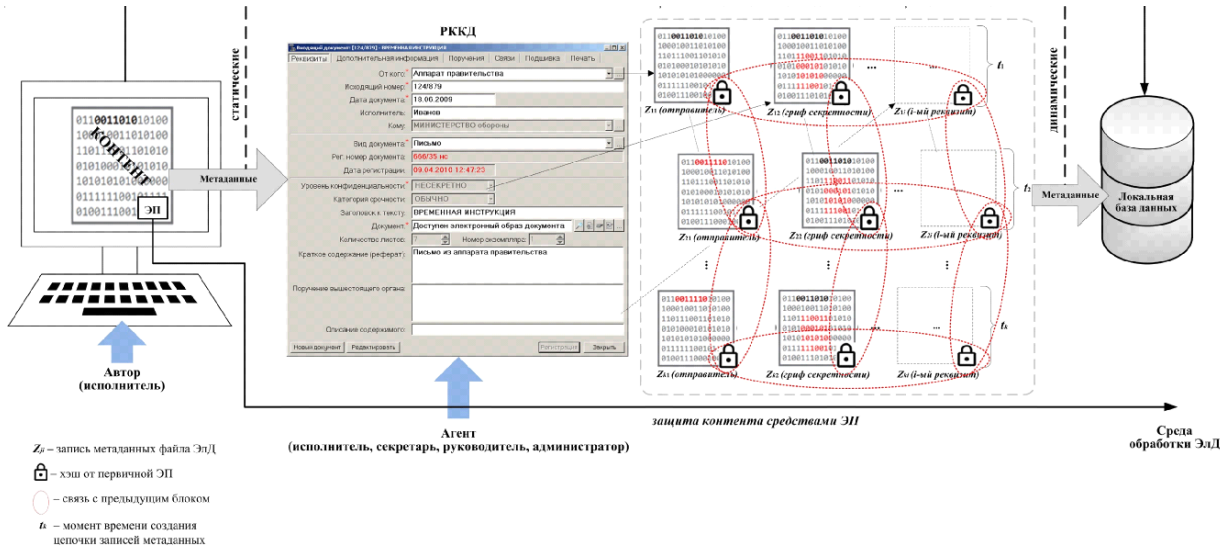


Рисунок 2.7. Концептуальне представлення моделі формування метаданих ЕД .

На основі цієї технології будується ланцюжок довіри криптографічна рекурсивна двовимірна послідовність метаданих ЕД, що є зв'язком із попереднім блоком після проведеної транзакції зміни метаданих у РККД, щоб інформацію усередині транзакцій не можна було підробити, кожна транзакція усередині блоку зазнає змін у метаданих, а потім - у метаданих, які не можна було підробити, кожна транзакція усередині блоку зазнає змін у РККД. Послідовності метаданих ЕД, починаючи з того моменту часу, у який було внесено зміни, неможливо.

Метою пропонованого технічного рішення є підвищення рівня захищеності метаданих ЕЛД, що обробляються АІС ЕД, з можливістю контролю їхньої цілісності, а також виявлення та локалізації номерів несанкціоновано модифікованих записів метаданих, у разі порушення їхньої цілісності уповноваженими користувачами (інсайдерами). Дане технічне рішення здійснюється таким чином.

Відбувається розбиття множини ключів K_U на дві підмножини: $K_U \in \{K_U^{(1)}, K_U^{(2)}, K_U^{(3)}\}$ і $K_U^* \in \{K_U^{*(1)}, K_U^{*(2)}, K_U^{*(3)}\}$, які містять три групи ключів, а саме $K_U^{(1)}$ - внутрішні системні ключі, $K_U^{(2)}$ - зовнішні ключі адміністратора, $K_U^{(3)}$ - зовнішні ключі оператора системи. На рисунку 2.8 представлено схему розбиття множини ключів K_U

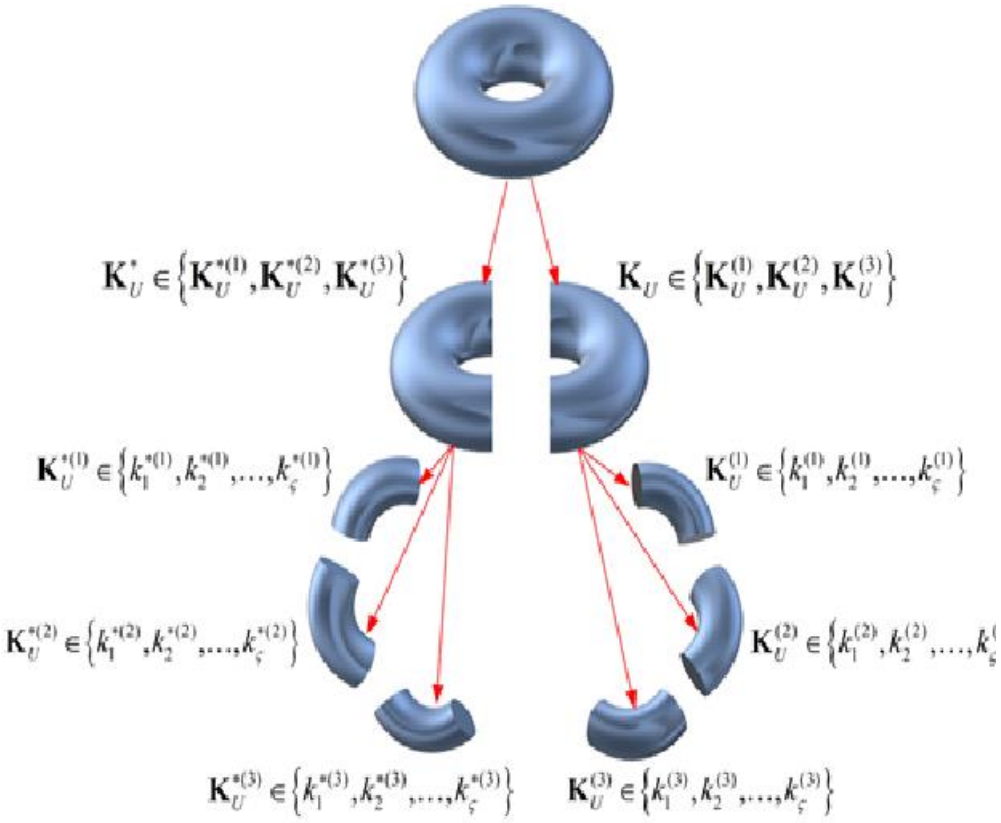


Рисунок 2.8. Схема розбиття множини ключів K_U

На рисунку 2.9 представлено функціональну схему криптографічного 2-D контролю цілісності метаданих ЕД, які обробляються автоматизованими інформаційними системами електронного документообігу.

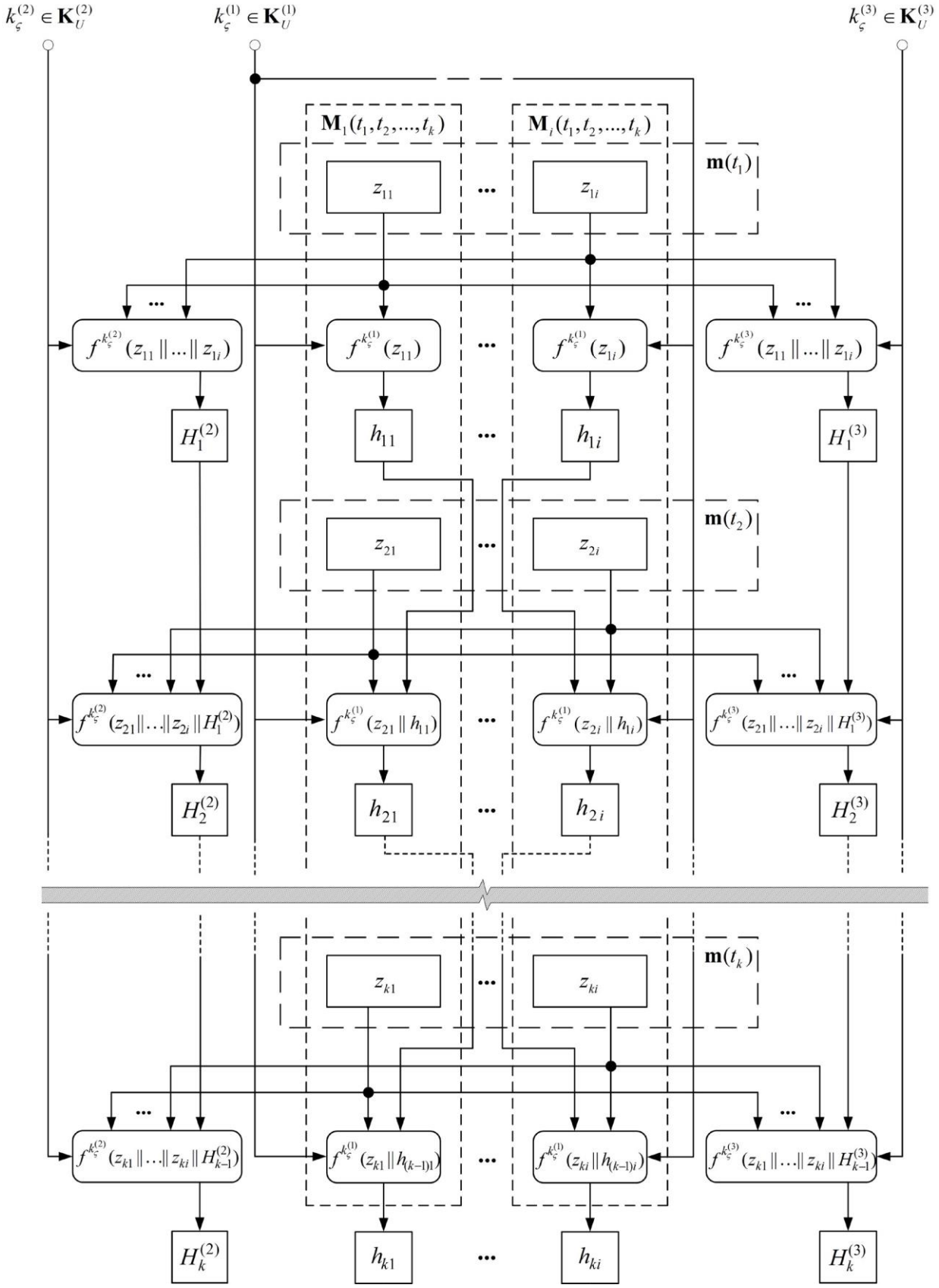


Рисунок 2.9. Функціональна схема криптографічного 2-D контролю цілісності метаданих ЕД, які обробляються автоматизованими інформаційними системами електронного документообігу.

На рисунку 2.10 представлено схему, яка пояснює виконання операцій криптографічного перетворення метаданих ЕД.

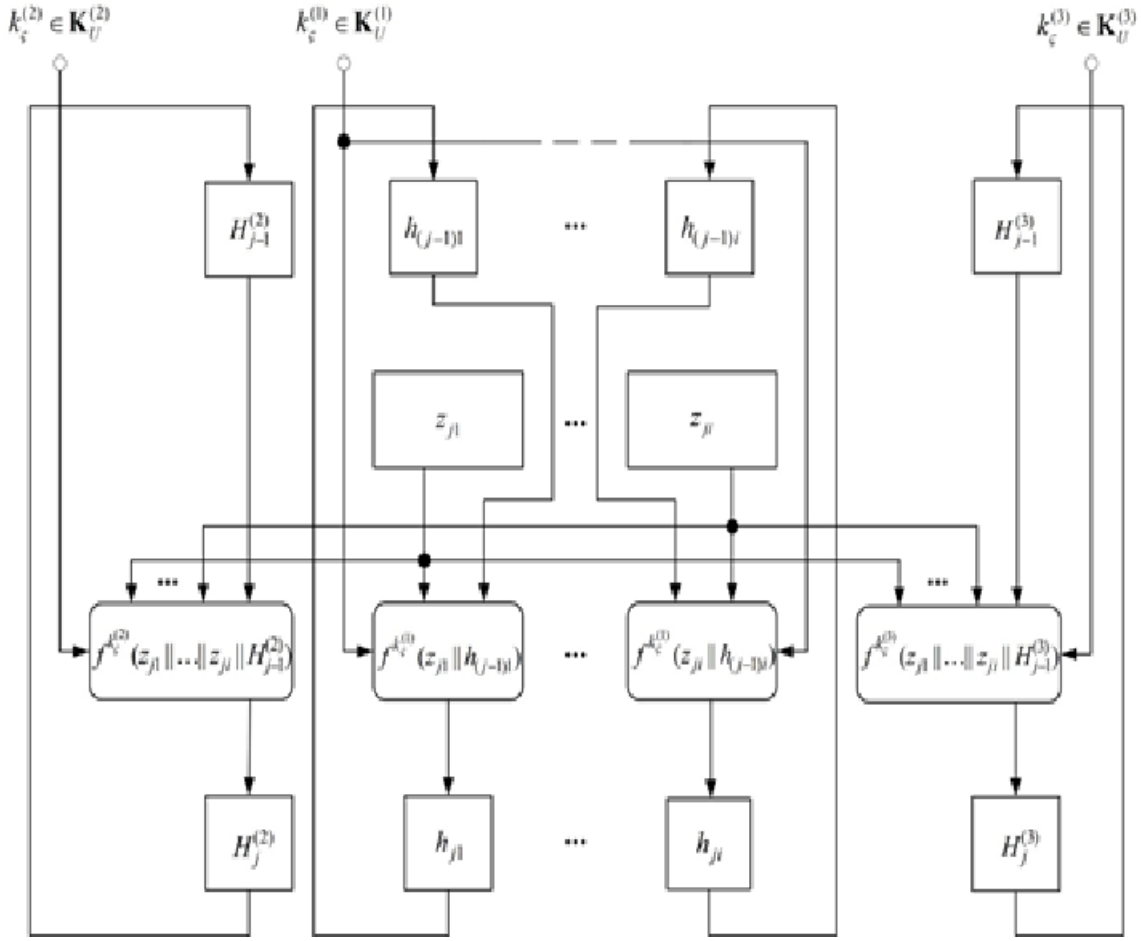


Рисунок 2.10. Схема, яка пояснює виконання операцій криптографічного перетворення метаданих ЕД.

На рисунку 2.11 представлено варіант реалізації функції криптографічного перетворення $f^{k_\varsigma^{(q)}}(\bullet|\,|\bullet)$ за рахунок ключів хеш-функції.

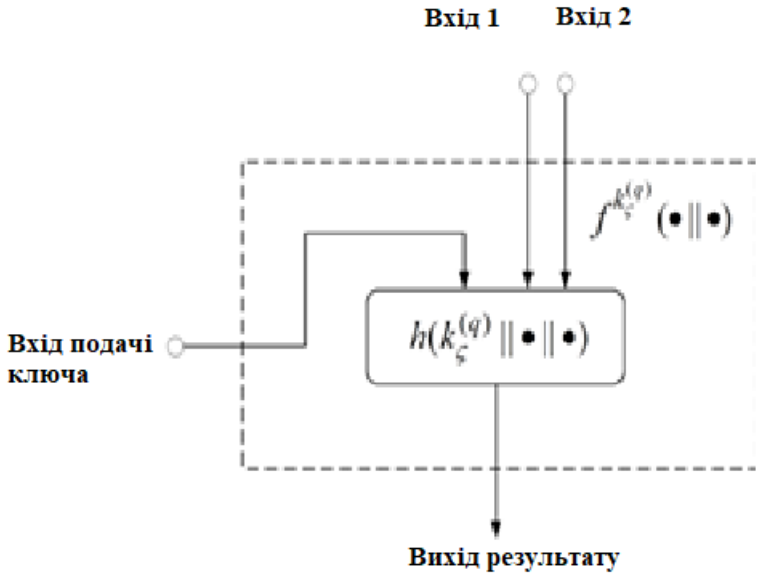


Рисунок 2.11. Варіант реалізації функції криптографічного перетворення $f^{k_\varsigma^{(q)}}(\bullet|\ |\bullet)$ за рахунок ключів хеш-функції.

В таблиці 2.1 представлено дані, які збережені записи метаданих та їх значення сигнатур.

Таблиця 2.1.

Моменти часу t редагування метаданих	**Записи метаданих та значення сигнатур**		
	На внутрішніх ключах системи $k_\varsigma^{(1)} \in \mathbf{K}_U^{(1)}$	**На зовнішніх ключах адміністратора** $k_\varsigma^{(2)} \in \mathbf{K}_U^{(2)}$	**На зовнішніх ключах оператора** $k_\varsigma^{(3)} \in \mathbf{K}_U^{(3)}$
t_1	z_{11} ... z_{1i} h_{11} ... h_{1i}	z_{11} ... z_{1i} $H_1^{(2)}$	z_{11} ... z_{1i} $H_1^{(3)}$
t_2	z_{21} ... z_{2i} h_{21} ... h_{2i}	z_{21} ... z_{2i} $H_2^{(2)}$	z_{21} ... z_{2i} $H_2^{(3)}$
⋮	⋮	⋮	⋮
t_k	z_{k1} ... z_{ki} h_{k1} ... h_{ki}	z_{k1} ... z_{ki} $H_k^{(2)}$	z_{k1} ... z_{ki} $H_k^{(3)}$

На малюнку 2.12 представлено варіант реалізації функції криптографічного перетворення $f^{k_\zeta^{(q)}}(\bullet|\,|\bullet)$ за рахунок електронного підпису.

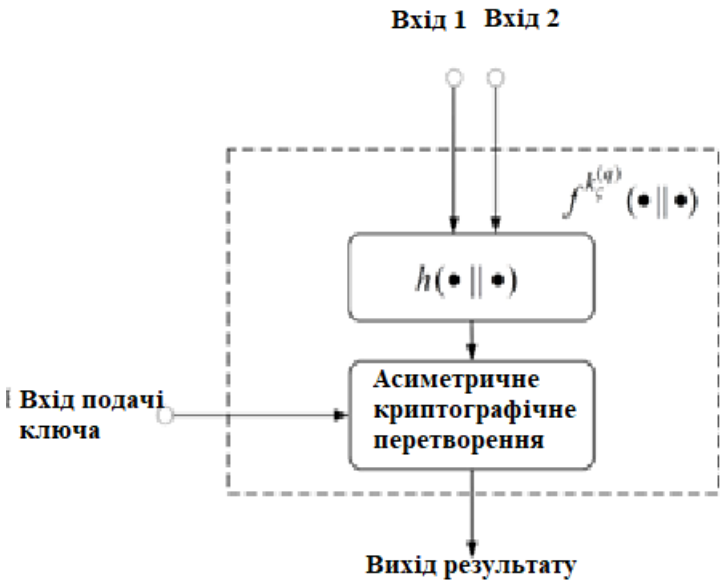


Рисунок 2.12. Варіант реалізації функції криптографічного перетворення $f^{k_\zeta^{(q)}}(\bullet|\,|\bullet)$ за рахунок електронного підпису.

На рисунку 2.13 представлено комутативну діаграму контролю цілісності метаданих ЕД для поелемнтного запису метаданих.

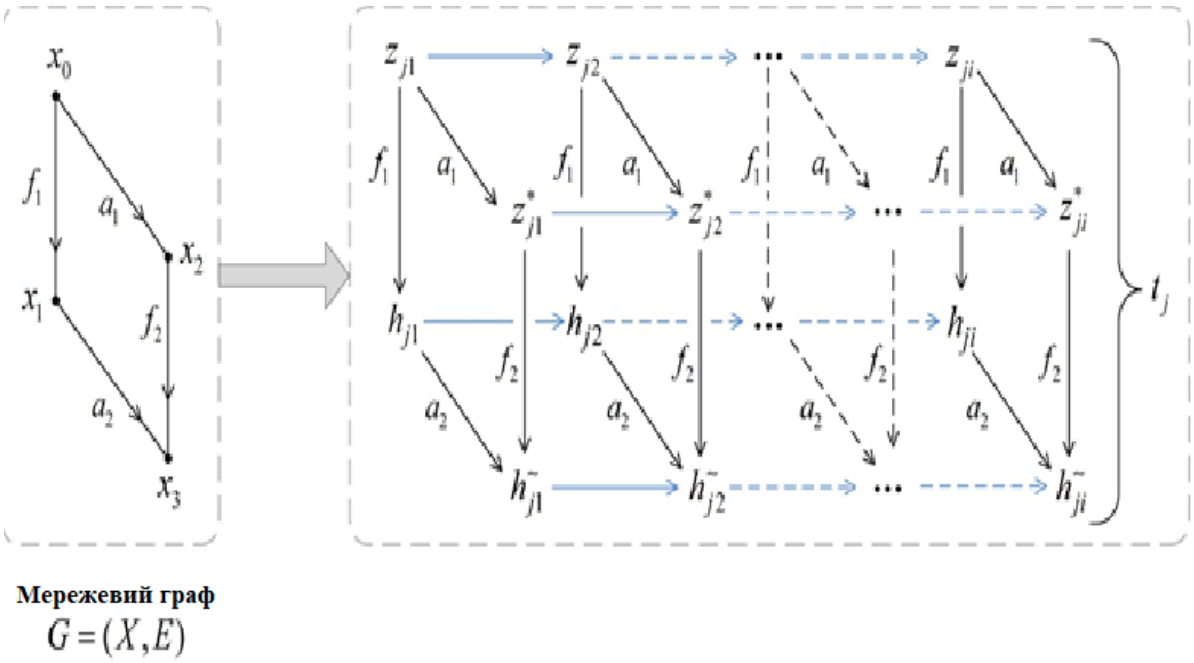


Рисунок 2.13. Комутативну діаграму контролю цілісності метаданих ЕД для поелемнтного запису метаданих.

На рисунку 2.14 представлено діаграму контролю цілісності метаданих ЕД для строк запису метаданих

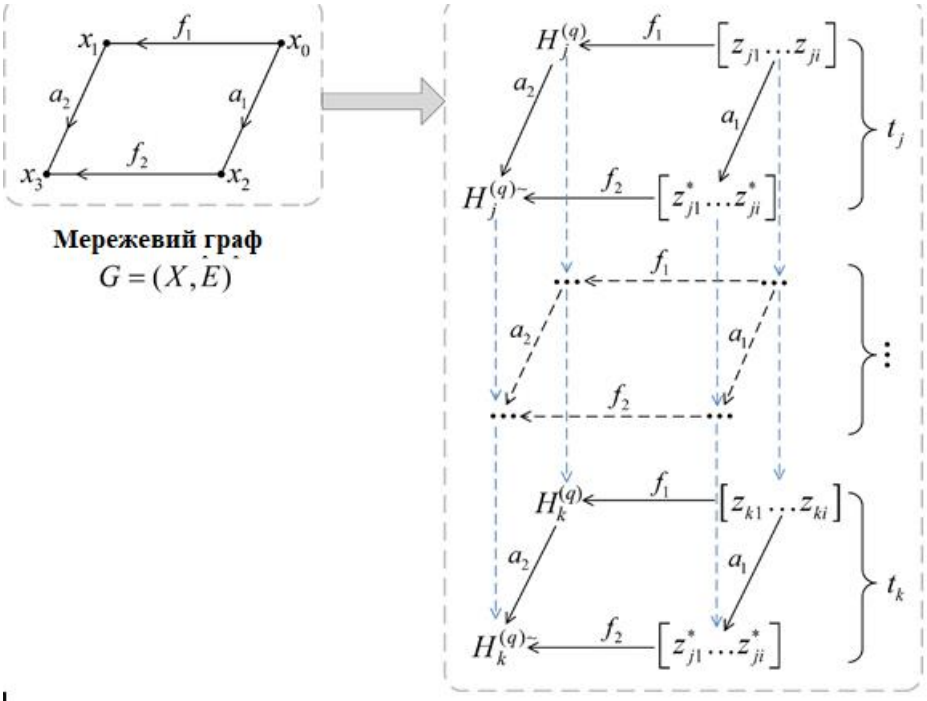


Рисунок 2.14. Діаграма контролю цілісності метаданих ЕД для строк запису метаданих.

2.2. Комплекс алгоритмів

Відповідно до стандарту з управління документами, ЕЛД складаються з контенту і метаданих, які описують контекст, контент і структуру документів, а також управління ними протягом часу. Метадані є критично важливою інформацією, яка циркулює в АІС ЕД і безпосередньо впливає на її функціональні можливості, що зумовлює необхідність ухвалення адекватних заходів щодо їх захисту від можливих несанкціонованих змін.

Наразі захист ЕЛД, оброблюваних АІС ЕД, забезпечує підсистема захисту інформації. Інформація при цьому зберігається в локальній базі даних, що захищається за допомогою розмежування доступу, а захист контенту ЕЛД, крім того, забезпечується засобами електронного підпису. Впливати на контент ЕлД може тільки автор, а на метадані ЕлД - усі, хто виконує функції агента, що не

виключає можливості внутрішніх порушень встановленої політики безпеки, які виражаються в порушенні функцій управління документами.

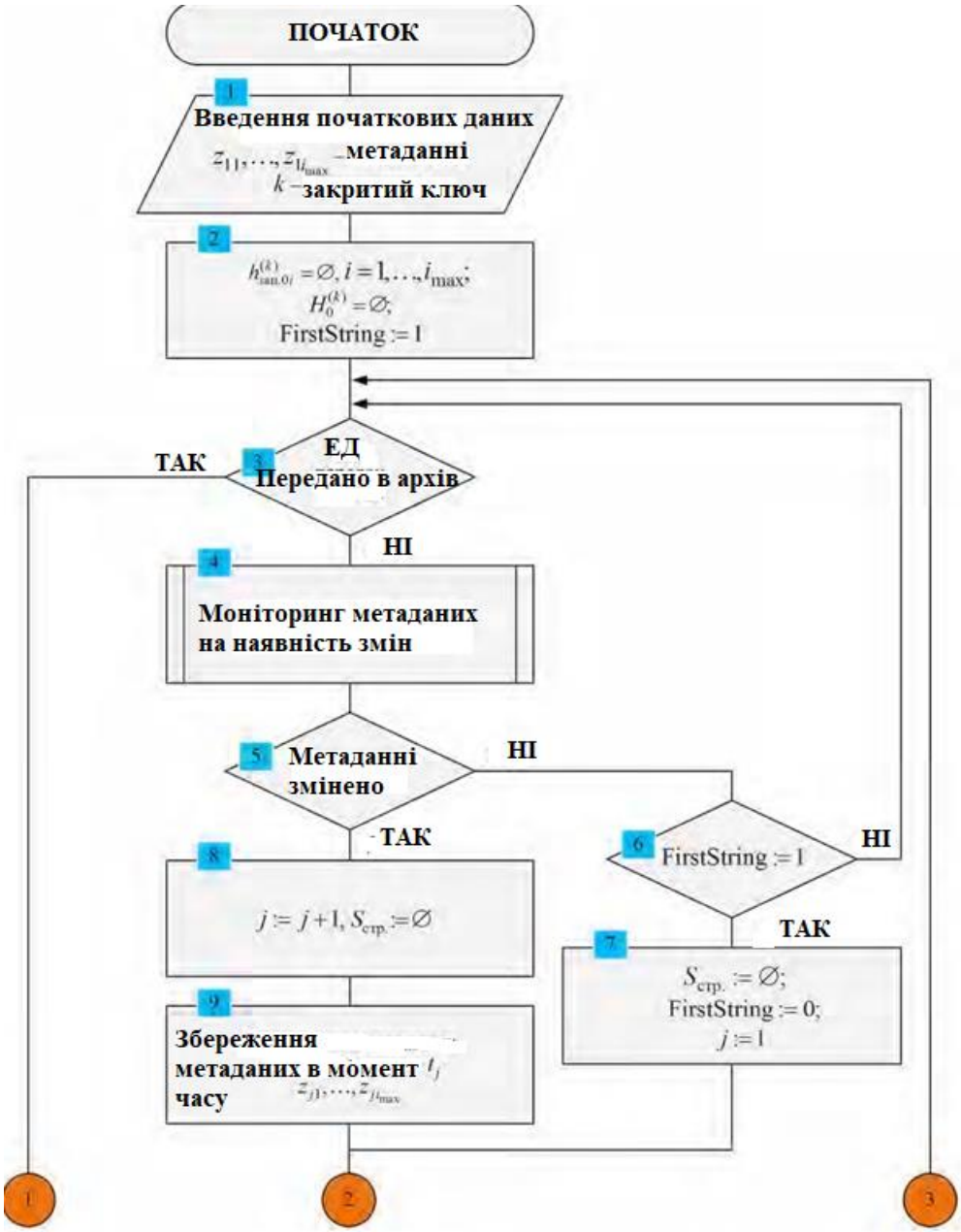
Саме застосування електронного підпису, що ґрунтується на криптографічних методах, дає змогу забезпечити необхідний рівень довіри до ЕЛД і, як наслідок, його правовий статус.

Таким чином, виникає низка протиріч:

- між результативністю захисту метаданих ЕЛД криптографічними методами та існуючими механізмами захисту (розмежування доступу) в умовах реалізації уповноваженими користувачами (інсайдерами) деструктивних впливів на АІС ЕД;
- між необхідністю реалізації алгоритмів криптографічного захисту метаданих, оскільки їх потрібно захистити від втрати або несанкціонованого видалення і зберегти або знищити згідно зі встановленими вимогами, і відсутністю таких алгоритмів у наявному науково-методичному апараті захисту метаданих ЕД. Обмеження і допущення:

- засоби захисту інформації, що функціонують в АІС ЕД, можуть мати вразливості, що сприяє їх використанню внутрішнім порушником у своїх цілях;
- внутрішнім порушником є адміністратор або уповноважений користувач, як унаслідок умисних дій, так і внаслідок помилок, спричинених людським фактором.

На рисунку 2.15 представлено блок-схему алгоритму формування криптографічної рекурсивної 2-D послідовності метаданих.


ПОЧАТОК
1
Введення початкових даних
$z_{11},\ldots,z_{1i_{max}}$ –метаданні
k –закритий ключ
2
$h^{(k)}_{зап.0i}=\varnothing, i=1,\ldots,i_{max};$
$H^{(k)}_0=\varnothing;$
FirstString := 1
3
ЕД
Передано в архів
ТАК
НІ
4
Моніторинг метаданих
на наявність змін
5
Метаданні
змінено
НІ
ТАК
6
FirstString := 1
НІ
ТАК
7
$S_{стр.}:=\varnothing;$
FirstString := 0;
$j:=1$
8
$j:=j+1, S_{стр.}:=\varnothing$
9
Збереження
метаданих в момент t_j
часу
$z_{j1},\ldots,z_{ji_{max}}$
1
2
3

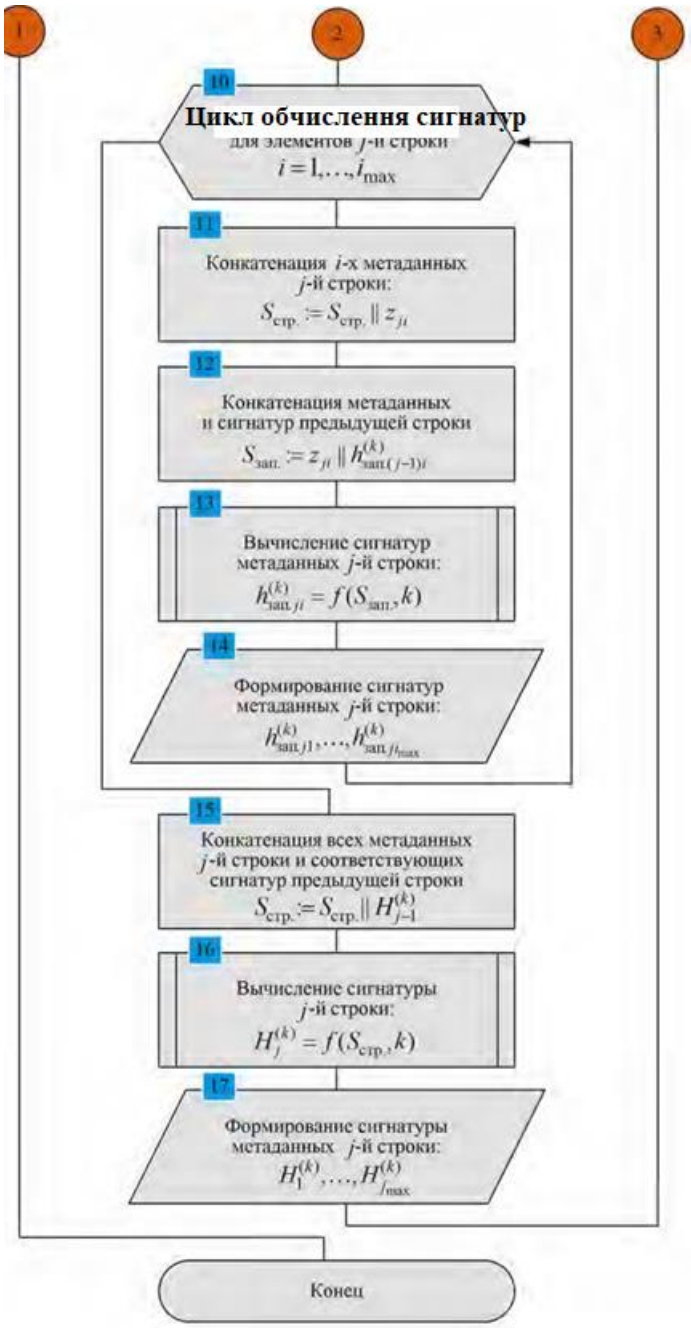
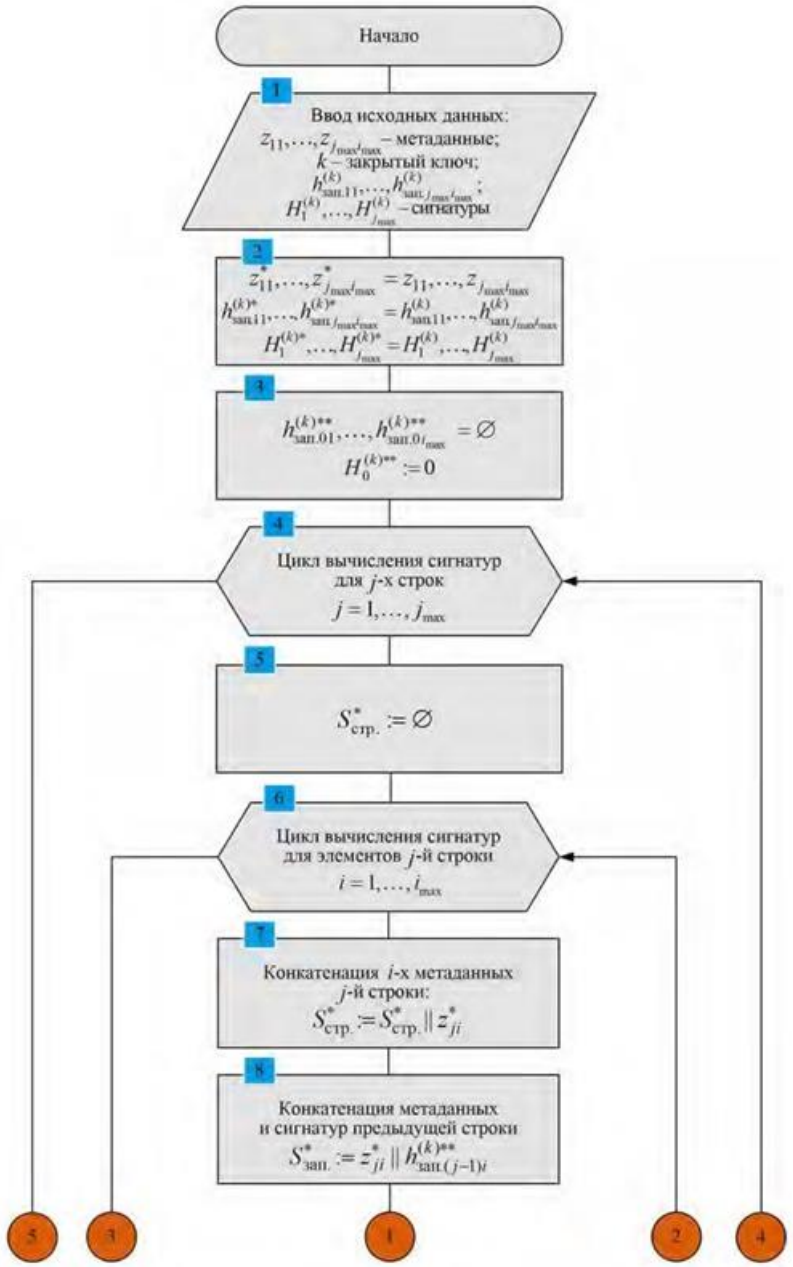


Рисунок 2.15. Блок-схема алгоритму формування криптографічної рекурсивної 2-D послідовності метаданих.

На рисунку 2.16 представлено блок-схему алгоритму перевірки криптографічної рекурсивної 2-D послідовності метаданних.


Начало
1
Ввод исходных данных:
$z_{11},\ldots,z_{j_{max}i_{max}}$ – метаданные;
k – закрытый ключ;
$h^{(k)}_{зап.11},\ldots,h^{(k)}_{зап.j_{max}i_{max}}$;
$H^{(k)}_1,\ldots,H^{(k)}_{j_{max}}$ – сигнатуры
2
$z^*_{11},\ldots,z^*_{j_{max}i_{max}} = z_{11},\ldots,z_{j_{max}i_{max}}$
$h^{(k)*}_{зап.i1},\ldots,h^{(k)*}_{зап.j_{max}i_{max}} = h^{(k)}_{зап.11},\ldots,h^{(k)}_{зап.j_{max}i_{max}}$
$H^{(k)*}_1,\ldots,H^{(k)*}_{j_{max}} = H^{(k)}_1,\ldots,H^{(k)}_{j_{max}}$
3
$h^{(k)**}_{зап.01},\ldots,h^{(k)**}_{зап.0i_{max}} = \varnothing$
$H^{(k)**}_0 := 0$
4
Цикл вычисления сигнатур для j-х строк
$j = 1,\ldots,j_{max}$
5
$S^*_{стр.} := \varnothing$
6
Цикл вычисления сигнатур для элементов j-й строки
$i = 1,\ldots,i_{max}$
7
Конкатенация i-х метаданных j-й строки:
$S^*_{стр.} := S^*_{стр.} \| z^*_{ji}$
8
Конкатенация метаданных и сигнатур предыдущей строки
$S^*_{зап.} := z^*_{ji} \| h^{(k)**}_{зап.(j-1)i}$
5
3
1
2
4

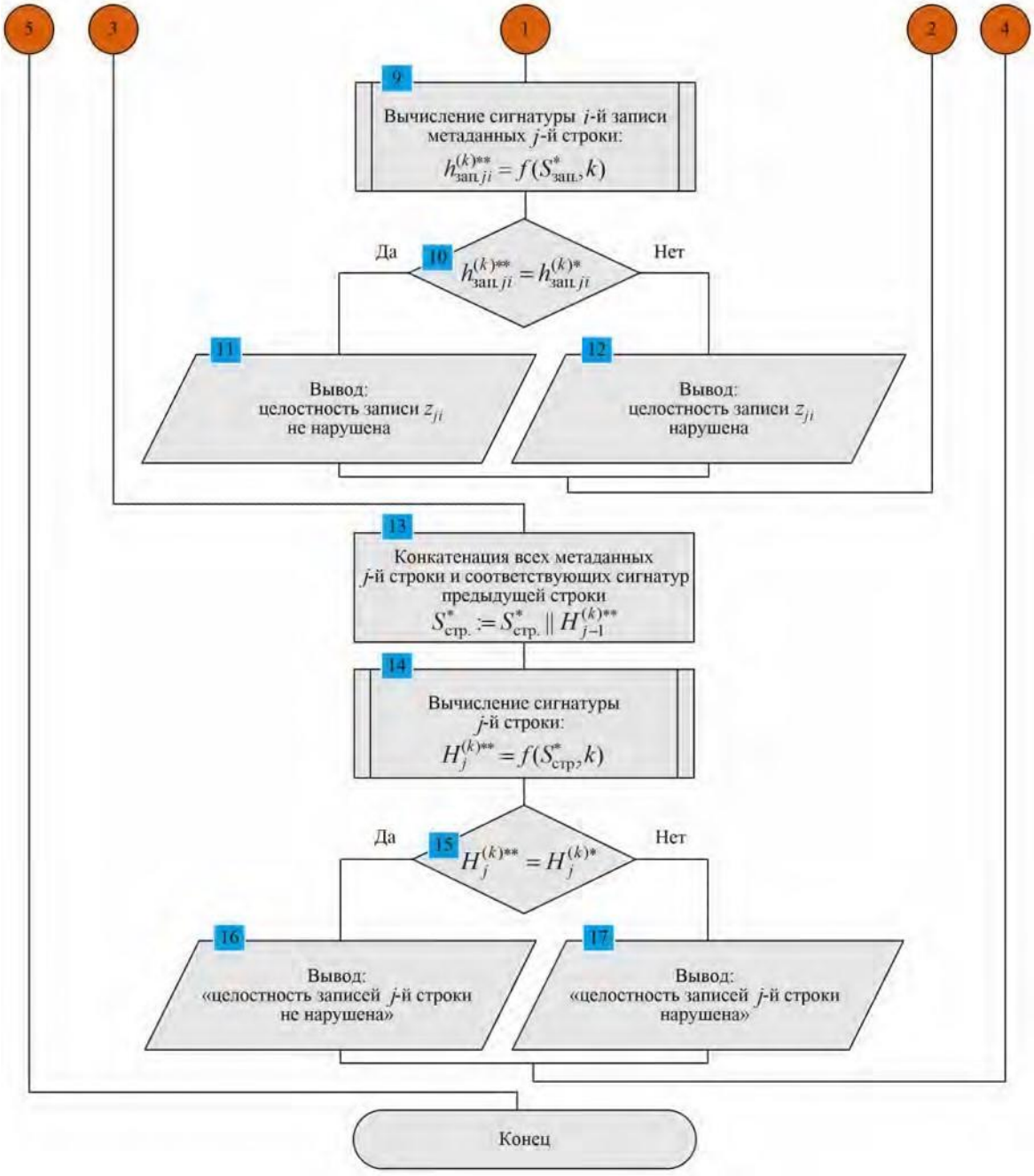


Рисунок 2.16. Блок-схема алгоритму перевірки криптографічної рекурсивної 2-D послідовності метаданих.

2.3. Методика застосування

У загальному вигляді управління документами включає в себе 4 етапи:
1) створення документа;

2) введення документа в систему з метою доведення ведення будь-якої діяльності;

3) вжиття належних заходів щодо захисту документа, в умовах мінливої в часі обстановки;

4) санкціоноване знищення або передача документа в архів.
При цьому метаданими документа слід управляти, як і самим документом, оскільки вони мають бути захищені від втрати або несанкціонованого видалення та збережені або знищені відповідно до вимог, визначених на основі аналізу проведеної діяльності. Таким чином, метадані є критично важливою інформацією, яка циркулює в АІС ЕД і безпосередньо впливає на її функціональні можливості, що зумовлює необхідність ужиття адекватних

заходів щодо їх захисту від можливих деструктивних впливів.

Рисунок 2.17. Схема процесу керування електронним документом.

ВИСНОВОК

1.Контроль цілісності метаданих розглянуто як складову частину процесу з управління ЕЛД у рамках вжиття належних заходів щодо захисту документа в умовах обстановки, що змінюється в часі.

2.Використання принципу ланцюгового запису даних у розв'язанні поставлених завдань дало змогу забезпечити технічні можливості з локалізації

несанкціоновано модифікованих записів метаданих, а також організувати взаємний контроль над діями уповноважених користувачів АІС ЕД.

3.Рішення, запропоноване в даній статті, є логічним продовженням раніше виконаних авторами досліджень у сфері аналізу та синтезу перспективних систем юридично значущого електронного документообігу та орієнтоване на реалізацію, переважно, у відомчих АІС ЕД .

4.Отримані результати, у поєднанні з багатовимірним поданням даних, дають змогу надійно захистити метадані, забезпечивши водночас ефективність управління ЕЛД, оброблюваними АІС ЕД.

5.У представленому рішенні ланцюговий запис даних є "надбудовою" над класичною базою даних, у ролі якої виступають метадані, представлені у вигляді багатовимірної моделі.

6.Такий підхід дасть змогу регламентувати порядок подання інформації, що зберігається в базі даних, ефективно використовувати розроблений механізм контролю цілісності метаданих, а також визначити порядок внесення, фіксації та відстеження змін.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ ТА ДЖЕРЕЛ

1. A. Suliman, M. K. Shankarapani, S. Mukkamala and A. H. Sung. RFID malware Cards and security devices for personal identification — Contactless proximity objects — Part 2: Radio frequency power and signal interface [Електронний ресурс] // ISO/IEC 14443-2:2020. – 2020. – Режим доступу до ресурсу: https://www.iso.org/standard/73597.html.

2. Guidelines for RFID-based Electronic Article Surveillance [Електронний ресурс]. – 2009. – Режим доступу до ресурсу: https://www.rfidjournal.com/gs1-releases-guidelines-for-rfid-based-electronic-article-surveillance.

3. IDTechEx: RFID System Frequencies. An overview of RFID frequencies for chip based tags. [Електронний ресурс]. – 2004. – Режим доступу до ресурсу: http://www.idtechex.com/.

4. L. Avanco, A. E. Guelfi, E. Pontes, A. A. A. Silva, S. T. Kofuji and F. Zhou. An effective intrusion detection approach for jamming attacks on RFID systems. International EURASIP Workshop on RFID Technology (EURFID); 2015; Rosenheim, Germany. p. 73–80.

5. Methodology for Evaluating Security in Commercial RFID Systems / T.M. Fernández-Caramés, P. Fraga-Lamas, M. Suárez- Albela, L. Castedo., 2017.

6. OpenPCD Reader [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://www.meriac.com.

7. Vogt H. Efficient Object Identification with Passive RFID Tags / Harald Vogt. – Zürich: Department of Computer ScienceSwiss Federal Institute of Technology (ETH), 2002. – 98 с

8. Y. Fu, C. Zhang and J. Wang. A research on Denial of Service attack in passive RFID system. In: International Conference on Anti-Counterfeiting Security and Identification in Communication (ASID); 2010; Chengdu, China. p. 24–28.

9. Fragmentation attacks. In: International Symposium on Collaborative Technologies and Systems; 2008; Irvine, United States.

10. Агафьин С. С. LW-КРИПТОГРАФИЯ: ШИФРЫ ДЛЯ RFID-СИСТЕМ / С. С. Агафьин // Безопасность информационных технологий / С. С. Агафьин., 2011. – С. 30–33.

11. Гнатюк М. А. ДИФРАКЦИЯ ЭЛЕКТРОМАГНИТНОЙ ВОЛНЫ НА КАСКАДНОМ СОЕДИНЕНИИ ПРЯМОУГОЛЬНЫХ ВОЛНОВОДОВ / М. А. Гнатюк, В. М. Морозов, С. В. Марченко. // ХНУРЕ. – 2019. – №196. – С. 130–137.

12. Горбачов В. Е. ОБЗОР ПРОБЛЕМ БЕЗОПАСНОСТИ И ПРОЕКТИРОВАНИЯ ЗАЩИЩЕННЫХ ЭЛЕКТРОННЫХ СИСТЕМ / В. Е. Горбачов, К. Б. Абдулрахман. // ХНУРЕ. – 2017. – №191. – С. 113–119.

13. Горбенко І. Д. ДОСЛІДЖЕННЯ СТРУКТУРИ СПЕКТРІВ СИГНАЛОВ З ЛІНІЙНОЮ ЧАСТОТНОЮ МОДУЛЯЦІЄЮ / І. Д. Горбенко, О. А. Замула. // ХНУРЕ. – 2018. – №193. – С. 192–198.

14. Горбенко І. Д. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ПОМЕХОЗАЩИЩЕННОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ РАЗЛИЧНЫХ ВНУТРЕННИХ И ВНЕШНИХ ВОЗДЕЙСТВИИ / І. Д. Горбенко, А. А. Замула, В. Л. Морозов. // ХНУРЕ. – 2017. – №189. – С. 5–14.

15. Горбенко Ю. І. УДОСКОНАЛЕНИЙ МЕХАНІЗМ ОДНОРАЗОВИХ КЛЮЧІВ ДЛЯ ПОСТКВАНТОВОГО ПЕРІОДУ НА ОСНОВІ ГЕШ-ФУНКЦІЙ [Електронний ресурс] / Ю. І. Горбенко, К. В. Ісірова // ХНУРЕ. – 2017. – Режим доступу до ресурсу: https://nure.ua/wp content/uploads/2017/Scientific_editions/191/5.pdf.

16. Описание процесса радиочастотной идентификации [Електронний ресурс] – Режим доступу до ресурсу: http://asupro.com/gps-gsm/meansidentification/reference/description-process-rfid.html.

17. Сальников Д. С. МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ДЛЯ БЕСПРОВОДНЫХ СИСТЕМ СВЯЗИ МИЛЛИМЕТРОВОГО ДИАПАЗОНА ВОЛН / Д. С. Сальников, А. І. Цопа. // ХНУРЕ. – 2018. – №192. – С. 140–148.

18. Шарфельд Т. Системы RFID низкой стоимости / Т. Шарфельд. – Москва, 2006. – 197 с.